Certificates, an introduction

Greg Rose
Ir. Ivana Belgers
• Some public key background
• The problem: trust
  – E-mail traffic
  – Surfing on the web
• Digital Certificates
  – Theory
  – CAcert
• Some examples from real life
• Your own CAcert certificate
Public key Crypto

• Also called “asymmetric”
• Keys come in pairs; keep one half secret
  – can’t derive the secret one from the public one
• Solves the key distribution problem… just publish the public keys
Public key Crypto

• Neat, we’re done, right?
  – Oops, no.

• Replaces it with the authentication problem
  – How do you know that the key belongs to who you think it does? Still a research problem.
Hybrid systems

• Often use a combination of Public, symmetric and no-key cryptography.
• e.g. SSL, SSH, PGP.
  – Public keys used for authentication, key exchange
  – Hash and public key for digital signature
  – Dynamic session key and classical cipher for security
  – Random numbers for all sorts of things.
Signatures

• With a piece of data, and a private key
  – you can sign things (signing)

• With a piece of data, a signature, and a public key
  – you can check that the corresponding private key made the signature, and
  – that the data is the same as when it was signed
  – (verification)
Certificates

- Just a blob of data that has been signed
- …except that the data tells you about
  - a public key
  - who that key belongs to
  - what they can do with it
  - for how long (validity)
  - and maybe other stuff

- Who signs it?
On the internet, nobody knows you’re a dog
PayPal example
Amazon.com

Dear Amazon member,

We regret to inform you that your Amazon account was been suspended for a period of 3-4 days, after that it will be terminated.

Your credit card on file with Amazon
Card number: XXXX-XXXX-XXXX-XXXX (Not shown for security purposes) Expiration date: XX/XX

Please sign in to your Amazon account and update your billing information:

http://www.amazon.com/gp/css/homepage.html

If your account information is not update, your account on Amazon will be terminated.

Thank you for your time!
Amazon Security Departament
Encryption (1)

Alice

Eve

Bob
Top ten reasons to rot-13 your USENET message:

10. Make people think you speak Yiddish
9. Foil the Prodigy censors
8. Make life difficult for the National Security Agency
7. Keep David Letterman from stealing your material
6. Make alt.conspiracy nervous
5. Because abjurer becomes nowhere, clerk becomes pyrex, and terra becomes green
4. Baffle newbies
3. It's cheaper than the Clipper Chip
2. America Online users can't decode your messages and find out what you're saying
1. Mom's on the Internet too
Disadvantages

- Sharing the secret
- Big keyring, many keys to protect
- Key exchange
- Not suitable for digital signatures

Advantage:
Relatively fast algorithm
Encryption (2)

Alice

Eve

Bob
Advantages

- Create keys for yourself
- One key pair per person
- Your public key can be... public
- Digital signatures are possible

Disadvantage:
Slow algorithms, big keys.
Implementations

• X.509
  – Hierarchical structure
    • Certificate Authority (CA)
    – Verisign, Thawte, ...

• PGP
  – Web of trust

• Support for E-mail and Web clients.
• Makes Digital Certificates
• Functions as a CA
• Free!
• Web-of-trust
• Began in Australia, now worldwide
  – 2000 certifiers, growing ± 150/month
  – 77000 certificates, growing ± 5000/month
In Practice (web)
De praktijk (e-mail)
And you?

- [http://www.cacert.org/](http://www.cacert.org/)
- Do your account registration, supply some private data
- [https://secure.cacert.org/cap.php](https://secure.cacert.org/cap.php)
- Print the form
- Find an assurer (or can be done by mail with notarized ID)
Questions?

• Questions?